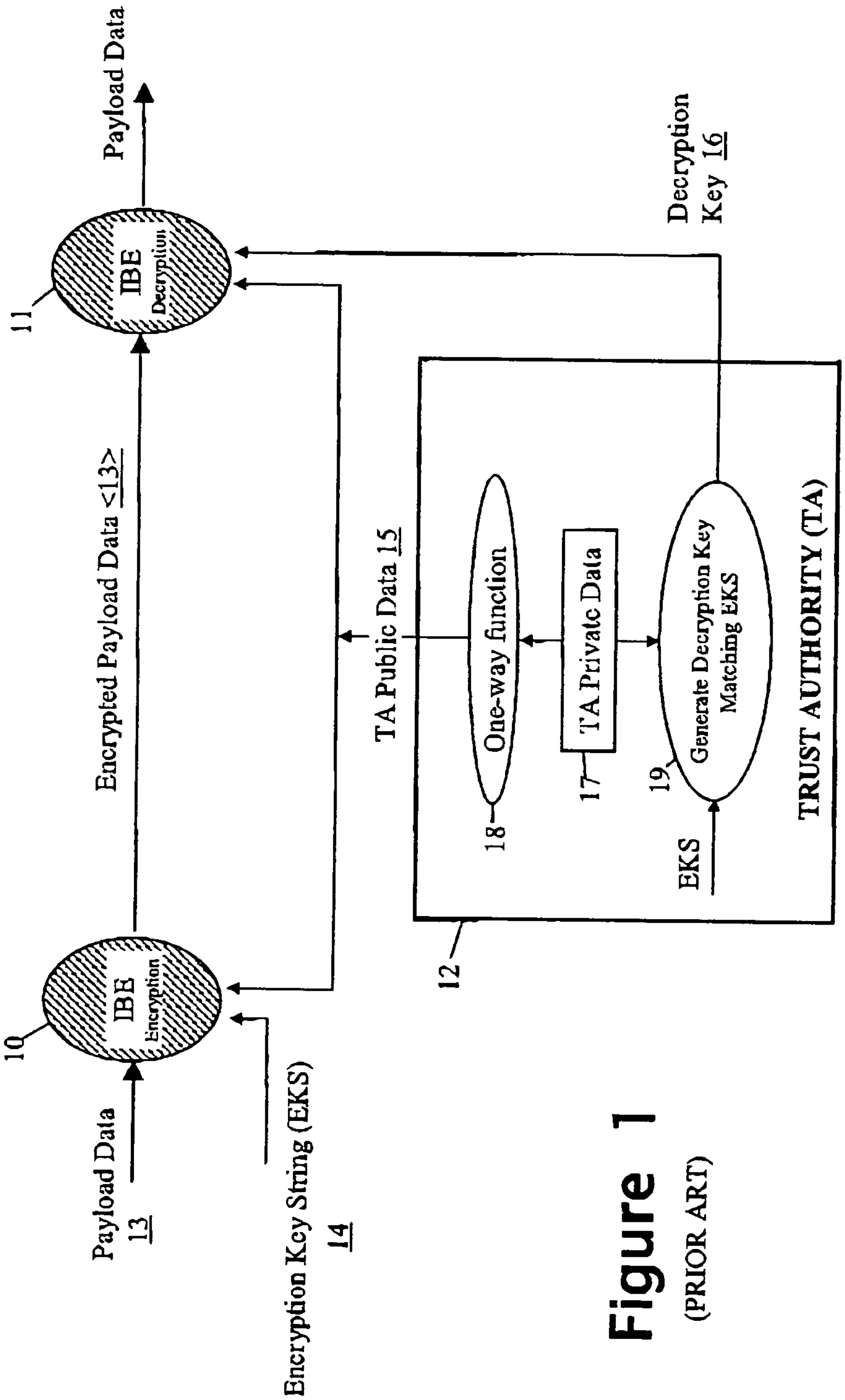
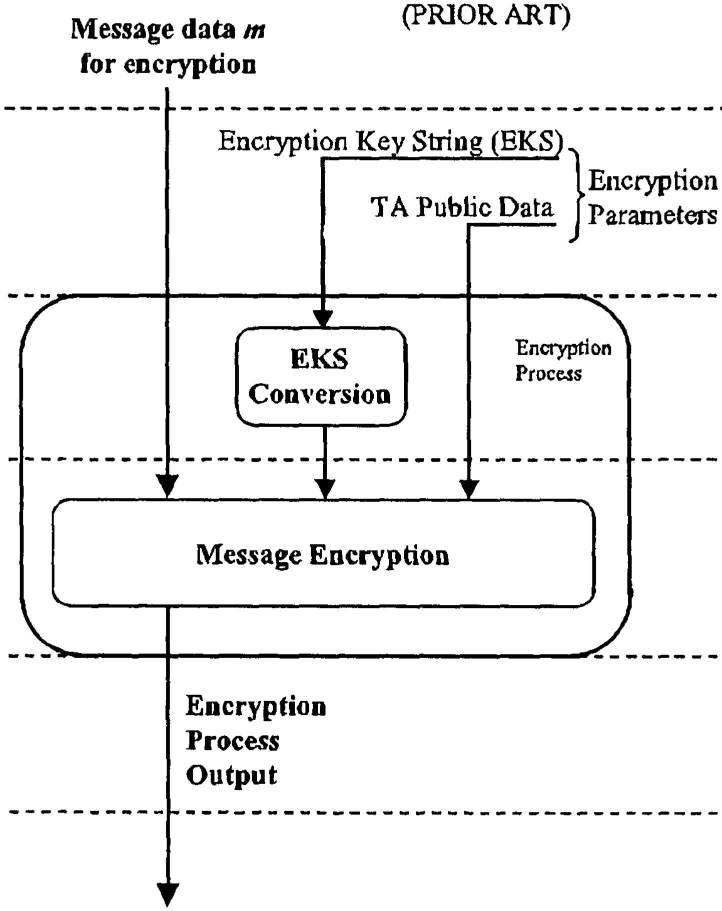


Figure 1
(PRIOR ART)

Figure 2

(PRIOR ART)



Identifier-Based Method		
Quadratic Residuosity	Bilinear Mappings $\wp : G_1 \times G_1 \longrightarrow G_2$	RSA Based
EKS Modulus N	EKS (P, sP) where P is in G_1, s is secret of TA	EKS Modulus n
$K = \#(\mathrm{EKS})$	"Map-to-point" hash $Q_{\mathrm{ID}} = H_1(\mathrm{EKS})$ where $H_1: \{0,1\}^* \longrightarrow G_1$	$e = \#(\mathrm{EKS}) \bmod n$
For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(\wp(sP, rQ_{\mathrm{ID}}))$ where: $H_2: G_2 \longrightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$
For each bit: s_+, s_-	$V, U (= rP)$	$m^e \bmod n$
(knowledge of EKS and TA concerned also needs to be available)		

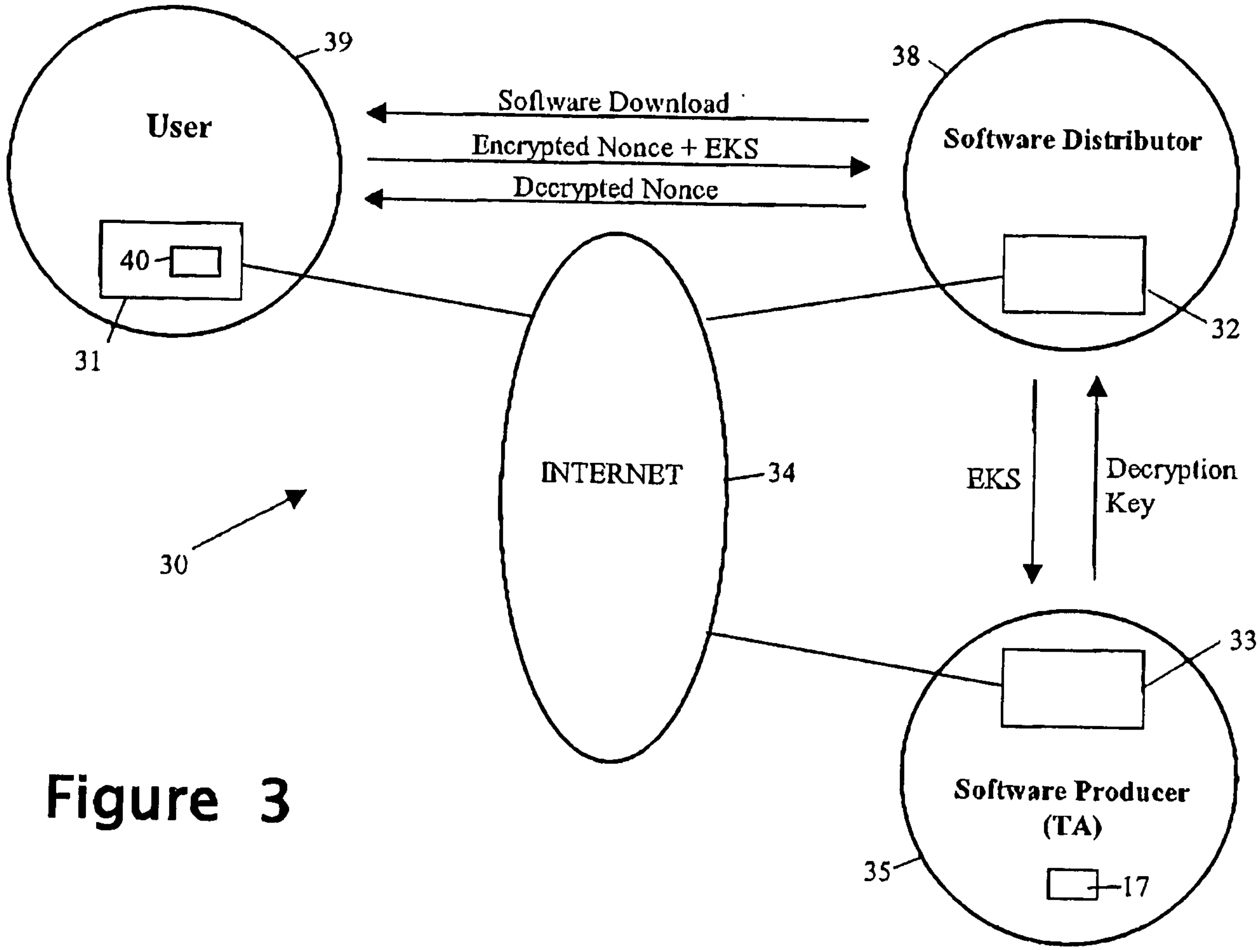

User
39
40
31
Software Download
Encrypted Nonce + EKS
Decrypted Nonce
Software Distributor
38
32
INTERNET
34
30
EKS
Decryption Key
Software Producer (TA)
33
35
17

Figure 3